Veteran Law Review
Volume: 9 Issue: 1
P-ISSN: 2655-1594 E-ISSN: 2655-1608

# Legal Protection for Consumers in Digital E-Commerce Agreements Based on the Civil Code and Consumer Protection Law

**Muhammad Reza Elia Habibullah[1]**

[1]*Faculty of Law, Surabaya State University,E-mail:* muhammadreza.23188@mhs.unesa.ac.id

**ARTICLE INFO**

**Keywords:**
*Digital Contract, Consumer Protection, e-commerce, Civil Code, GDPR.*

**How to cite:**
Habibullah, Muhammad Reza Elia. (2026). *Legal Protection for Consumers in Digital E-Commerce Agreements Based on the Civil Code and Consumer Protection Law.*
*Veteran Law Review.* 9(1). 12-27.

Received:2025-12-08
Revised:2026-05-26
Accepted:2026-06-02

**ABSTRACT**

*The digitalization of commercial transactions has significantly transformed the formation and enforcement of agreements between businesses and consumers. This study examines the legal validity of digital contracts in Indonesia under the Civil Code (KUH Perdata), "the Electronic Information and Transactions Law (UU ITE), and Government Regulation No. 71 of 2019", as well as their implications for consumer protection under the Consumer Protection Law (UUPK). Using a normative juridical and comparative method, the research finds that Indonesia recognizes electronic contracts and electronic signatures as legally binding, yet its regulatory framework remains fragmented and does not fully address key elements of digital consumer protection, such as product conformity, withdrawal rights, and mandatory software updates. A comparison with the Netherlands, a civil law country with a more advanced regulatory structure shows that Dutch law, supported by EU frameworks such as the GDPR and Consumer Rights Directive, provides stronger safeguards, clearer obligations for digital content providers, and more effective mechanisms for dispute resolution. The study concludes that although Indonesia has established a basic legal foundation for digital contracting, further regulatory development is required to respond to risks related to data breaches, online fraud, and cross-border e-commerce. Strengthening institutional capacity and harmonizing digital regulations are essential to enhancing consumer protection in the digital era.*

## 1. Introduction

The development of information technology has fundamentally changed the business world in recent decades. The digital revolution has brought about major changes in business, bringing new opportunities and complex challenges. One aspect that will be significantly affected by these changes is the process of signing, executing, and enforcing business contracts. The digital era has given rise to new business practices that are more efficient and globally connected. Business contracts are no longer limited to conventional forms that require physical signatures or face-to-face meetings between parties.

The digital era has had a major impact on the business competitive environment around the world. Commercial competition is considered more competitive, requiring adequate legal protection. Entrepreneurs must participate in and control the development of the digital era Entrepreneurs must participate in and control the development of the digital era in their business activities. Entrepreneurs utilize digital media in various forms to support marketing activities and improve production quality. Ultimately, the goal of businesses that use digital media is to increase market share. Business actors place advertisements in the form of videos, audio, or images. At the same time, in terms of increasing production, business actors share information about production methods with the wider community.

The rapid advancement of information technology has given rise to new legal aspects with the aim of ensuring legal justice, legal benefits, and legal certainty (Muhammad Erwin, 2012). A crucial legal aspect in technological development is the protection of various forms of agreements, which are becoming increasingly diverse (Hikmahanto Juwono, 2006). The various conveniences are regulated by the Civil Code (hereinafter referred to as the Civil Code).

The development of digital technology has brought significant changes in the pattern of legal relationships between businesses and consumers, particularly in the mechanism of contract formation. Previously, contracts were generally made in writing in the form of physical documents, but now transactions can be carried out digitally through various platforms, including instant messaging applications such as WhatsApp and other social media. This transformation has made transactions easier, but on the other hand, it has created new challenges related to compliance with consumer protection regulations. The phenomenon of contract violations in the context of consumer protection indicates a shift in regulatory compliance, where many businesses and consumers enter into digital contracts without understanding their validity or legal consequences. Prior to the enactment of the Electronic Information and Transactions Law, people who had used electronic contracts still relied on the Civil Code (KUHPdt) for legal protection.

Therefore, this study is important to explore the extent to which digital agreements can be considered legally valid and how legal protection for consumers can be realized if agreements are only made through digital means, such as WhatsApp conversations or other social media. This study is expected to contribute to the development of civil law understanding and consumer protection amid the rapid digital transformation.

## 2. Method

This study uses the normative legal research method, which focuses on analyzing the positive legal norms that govern the object of study. This approach was chosen because the issues under study relate to legal regulations concerning the validity of electronic agreements and consumer protection in digital transactions, both in the Indonesian legal system and in the legal framework of another country used for comparison, namely the Netherlands.

## 3. Main Heading of the Analysis or Results

A digital agreement is the process of exchanging goods, services, or information electronically using digital technology, such as the internet, smartphones, computers, or special applications, without involving physical cash. These transactions involve the real-time transfer of data and funds via the internet using secure and encrypted electronic payment systems. Unlike conventional agreements, which are usually signed on paper, digital agreements are created digitally using computers, the internet, or other electronic devices.

### 3.1. How does the validity of digital agreements affect consumer protection?

According to the Electronic Information and Transactions Law (ITE Law), electronic contracts have the same legal standing as conventional contracts, and are therefore legally valid as long as they meet certain requirements. The validity of an agreement is a fundamental aspect of contract law, because only valid agreements can have legal consequences for the parties involved. In Indonesian civil law, the requirements for a valid agreement are explicitly regulated in Article 1320 of the Civil Code, which contains four main elements: the existence of an agreement between the parties (achieved when the user clicks the Agree button, or clicks the "Create Account/Order/Checkout" button).

The ITE Law recognizes that electronic actions ("clicks") are a valid form of consent), legal competence (Platforms usually request age verification or a statement saying "I am 18+". If the user is still a minor, the agreement is at risk of being canceled. In e-commerce, the competence of buyers and sellers is the same as in ordinary agreements, only the medium is digital), specific object (must be clearly stated on the website or application display, such as item description, price, service, subscription duration, and rules of use; if the application is unclear about the object, the agreement may be considered chaotic/not fulfilling the specific object element), and lawful cause (digital agreements used for the sale and purchase of illegal goods such as drugs, weapons, stolen personal data, gambling, are automatically invalid). These four elements are divided into two categories, namely subjective requirements (agreement and competence) and objective requirements (specific object and lawful cause). If the subjective requirements are not met, then the agreement can only be requested to be canceled. Conversely, if the objective requirements are violated, then the agreement is null and void from the outset.

Advances in information technology have changed the face of transactions in Indonesia. Whereas contracts were previously understood as physical documents with wet signatures, electronic contracts are now an integral part of people's activities, from online shopping to the use of digital applications. To provide legal certainty, the government passed Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later revised through Law No. 19 of 2016. Through this regulation, the state recognizes that electronic documents, electronic signatures, and electronic contracts have the same legal force as conventional contracts.

Article 18 paragraph (1) of the ITE Law stipulates that electronic transactions made through electronic systems are valid and binding as long as they are based on the agreement of the parties. This means that Indonesian law formally recognizes electronic contracts, including clickwrap agreements, as long as the valid requirements for agreements under Article 1320 of the Civil Code are met. Technical provisions regarding electronic contracts are regulated in Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). Article 46 paragraph (2) of this PP emphasizes that electronic contracts are valid if there is an agreement between the parties, the parties are legally competent, the object is clear, and the purpose is lawful. Thus, GR 71 of 2019 explicitly integrates the requirements for a valid agreement under the Civil Code into the electronic realm, ensuring that classical civil law remains relevant in the digital age. GR 71 of 2019 also requires electronic system operators to store electronic contracts for a certain period of time and ensure their accessibility, given that many consumers find it difficult to access the terms and conditions they have agreed to. With this storage requirement, service providers cannot arbitrarily change or delete the contents of the agreement. This provision also strengthens the principle of legal certainty and protects consumers.

Digital transactions carry many risks, such as online fraud through phishing links, theft of personal data, and server disruptions that hinder transactions. Therefore, legal protection is a measure to provide security guarantees for legal subjects through various legal instruments, both preventive and punitive, and can be in the form of written or unwritten provisions. One regulation that plays an important role is Law No. 8 of 1999 concerning Consumer Protection (UUPK), which has contributed greatly to the development of the national legal system. This regulation affirms the objectives of law in the economic sphere, namely to build a healthy and competitive economy and market, while also serving as the main basis for determining the responsibility of business actors for losses suffered by consumers.

In practice, digital transactions carry a number of potential risks, including non-fulfillment of the agreement or incomplete fulfillment of performance, abuse of authority related to agreed decisions, damage or loss of goods, late delivery, and various other forms of uncertainty. These risks can cause losses for consumers. Based on Article 4 letter h and Article 7 letter g of the Consumer Protection Law, consumers are entitled to compensation or damages if the goods and/or services received do not comply with the agreement. The obligation to provide compensation must be fulfilled by the business operator if there is a discrepancy between the goods and/or services provided and the initial agreement. Therefore, legal protection is very important in digital agreements so that all parties involved can feel secure when conducting electronic transactions. The ITE Law includes provisions to protect personal data in electronic transactions. Electronic transaction operators are responsible for maintaining the confidentiality and integrity of personal data. If there is a leak or misuse of personal data, the person responsible will be punished in accordance with applicable laws. Then, the aggrieved party in a dispute involving a digital agreement has the right to take legal action. Based on the ITE Law, disputes can be resolved through court or arbitration. The court can assess the validity of a digital agreement by examining whether all valid agreement requirements have been met, such as agreement, legal competence, and the use of a valid electronic signature.

Legal Sanctions for Violations of Digital Agreements The ITE Law imposes sanctions on individuals who violate the requirements of electronic transactions, such as fraud, falsification of electronic documents, or violation of personal data privacy. Sanctions that may be imposed include imprisonment or fines, which are intended to deter offenders and ensure that those who have suffered losses are brought to justice.

"Article 11 Paragraph (1) of the 2008 ITE Law states that Electronic Signatures have legal force and legal effect as long as they meet the following requirements:

a. the data used to create the Electronic Signature is unique to the Signatory;
b. the data used to create the Electronic Signature during the electronic signing process is only in the control of the Signatory;
c. any changes to the Electronic Signature that occur after the time of signing can be detected;
d. any changes to the Electronic Information related to the Electronic Signature after the time of signing can be detected;
e. there is a specific method used to identify the Signatory; and
f. there is a specific method to indicate that the Signatory has given their consent to the related Electronic Information".

"Articles 5 and 6 of the ITE Law" emphasize that information, documents, and electronic signatures are legally valid as evidence in e-commerce transactions, as long as the data can be verified, downloaded, displayed, guaranteed to be complete, and accountable. This provision is clarified in the Explanation of Article 5 of Law Number 19 of 2016, which states "that electronic information and/or electronic documents have binding force and are recognized as valid evidence to provide legal certainty in the implementation of electronic systems and transactions, particularly in relation to the process of evidence and legal actions carried out through electronic media". This regulation emphasizes that even though it is in the form of a series of codes, an electronic signature has the same legal status as a conventional signature, and therefore has the same legal force and consequences.

"The Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), particularly Article 46", regulates in more detail and bindingly the validity and legal consequences of digital transactions. This provision gives equal legal force and more specific regulations to electronic agreements, thereby superseding or prioritizing the application of the general norms of Article 1320 of the Civil Code. Thus, although Article 1320 of the Civil Code forms the basis of the general principles of valid agreements, in the practice of digital transactions, the implementation and validity of agreements must first refer to the provisions of this Government Regulation as the relevant and more up-to-date norms. Article 46 of the PSTE Government Regulation clearly regulates the validity of electronic documents, including electronic agreements in online sales transactions, and

Veteran Law Review
Volume: 9 Issue: 1
P-ISSN: 2655-1594 E-ISSN: 2655-1608

stipulates that these documents are equivalent to conventional documents. Thus, electronic signatures serve as authentic evidence binding the parties and provide legal certainty for digital agreements. In electronic agreements, this agreement is realized through statements sent via electronic means such as email, applications, or websites.

The rights and obligations of business actors are regulated in "Law Number 8 of 1999 concerning Consumer Protection", specifically through the provisions of Articles 6 and 7. Meanwhile, Article 4 of the UUPK stipulates a number of consumer rights, including the right to comfort, safety, and security in using goods and/or services; the right to obtain representation, protection, and fair dispute resolution; the right to choose goods and/or services and receive those products in accordance with the promised exchange value, terms, and guarantees; the right to obtain accurate, understandable, and honest information about the conditions and guarantees of goods and/or services; and the right to express opinions and complaints regarding the products or services used.

### 3.2. How does consumer protection for digital transactions between civil law countries and Indonesia work?

Consumer protection in the Netherlands is regulated in Book 6 of the Civil Code, which governs consumer contracts and warranty for defects, and Book 7, which governs the sale of digital or physical goods. The Netherlands has implemented a legal framework that specifically regulates digital transactions. Since April 27, 2022, the country has adopted new provisions in the Dutch Civil Code (DCC), namely Title 7.1AA, which is designed to regulate contractual relationships related to the provision of digital content and digital services to consumers. Consumer protection regulations in the Netherlands generally originate from European Union legal instruments that are then transposed into national regulations and reinforced through domestic provisions in the Burgerlijk Wetboek or Civil Code.

Within its regulatory framework, Indonesia uses a regulatory model that is spread across various sectors. The Ministry of Trade is responsible for overseeing e-commerce and electronic trading activities, while the Financial Services Authority (OJK) oversees fintech services and technology-based lending providers. Bank Indonesia (BI) has authority over the regulation of payment systems, electronic money, and digital wallet services. The Ministry of Communication and Information Technology has the mandate to manage personal data protection since the enactment of Law Number 27 of 2022.

In contrast, the Netherlands, as part of the European Union, implements a more integrated and coordinated regulatory model with a clear division of functions. The Autoriteit Financiële Markten (AFM) acts as a conduct supervisor in the financial sector, while De Nederlandsche Bank (DNB) acts as a prudential supervisor that ensures the stability of the financial system. On the other hand, the Authority for Consumers and Markets (ACM) is tasked with supervising consumer protection in digital transactions, and the Autoriteit Persoonsgegevens (AP) is authorized to ensure compliance with GDPR provisions.

In electronic commerce, businesses operating through web shops are required to provide transparent information about the seller's identity, the specifications of the goods or services, the price including value added tax (VAT), payment methods, delivery terms, guarantees, and consumers' right to withdraw from the transaction. Furthermore, for digital contracts, the Netherlands applies provisions that digital products must meet conformity standards, including the obligation for merchants to provide adequate software and security updates. Consumers in the Netherlands are legally entitled to use the withdrawal right mechanism in remote transactions for a minimum of 14 days from the date the goods are received or from the date the digital service contract is agreed upon. This provision is not explicitly recognized in Indonesian law, as neither the UUPK nor the ITE Law contains provisions on a cooling-off period that is specifically intended for digital transactions.

In the event of a consumer dispute in Indonesia, consumers have the opportunity to file a complaint with the Consumer Dispute Settlement Agency (BPSK), either verbally or in writing. The complaint is then followed up by summoning the business operator and providing three options for resolution: conciliation, mediation, or arbitration. Decisions made through conciliation and mediation are final and binding, while arbitration decisions, based on PERMA No. 1 of 2006, can still be appealed to the District Court. Meanwhile, in the Netherlands, consumers can submit objections or complaints to the Authority for Consumers and Markets (ACM) for administrative law enforcement, to Consumentenbond for consumer advocacy, or to Geschillencommissie as an independent alternative dispute resolution (ADR) institution with the authority to issue binding decisions on the parties.

Regarding digital content and services, regulatory updates in 2022 emphasize that consumers have the right to obtain content or services that continue to meet quality standards, including the right to ongoing security updates. DCC Title 7.1AA stipulates that digital content or service providers must ensure that digital products have the quality and quantity that consumers expect and are in line with public statements from sellers or manufacturers, including the provision of necessary updates. Meanwhile, Indonesia's ITE Law focuses more on the legality of electronic documents and transactions, but does not comprehensively regulate consumer rights to conformity, updates, or platform provider accountability. In reality, personal data protection is still weak, consumer digital literacy is relatively low, and oversight mechanisms are not yet optimal.

In digital transactions, the security of personal data is a crucial issue due to the potential for misuse that could cause harm to consumers. Indonesia regulates this through Law No. 27 of 2022 on Personal Data Protection (PDP Law), which is in line with the European Union's General Data Protection Regulation (GDPR) standards. This regulation will come into full effect on October 17, 2024, and regulates the stages of acquisition, processing, and storage of personal data. E-commerce service providers are required to adjust their privacy policies, implement encryption on user data, and strengthen the security of cloud-based infrastructure. On the other hand, the Netherlands has directly adopted the GDPR as part of EU regulations and implemented it through the Dutch GDPR Implementation Act (UAVG / *Uitvoeringswet Algemene Verordening Gegevensbescherming*). The country has a more comprehensive data protection framework with a more established level of enforcement through the Dutch Data Protection Authority. The GDPR itself sets strict standards regarding consent mechanisms, expands the rights of data subjects, and imposes significant administrative penalties for violations, namely up to 4% of total global revenue or €20 million.

Compared to Indonesia, the Dutch regulatory framework shows a higher level of maturity. This is due to regulations that specifically cover digital transactions, including digital content, digital services, and goods with digital elements. The 2022 regulation is a concrete example of how consumer protection has been extended to digital products. In addition, the Netherlands has strong and proactive supervisory agencies, such as the Authority for Consumers and Markets (ACM) and the Netherlands Food and Consumer Product Safety Authority (NVWA), as well as clear guidelines for businesses in the e-commerce ecosystem. Consumer rights in online transactions, such as the 14-day withdrawal right and detailed information obligations, are also protection standards that are integrated with European Union regulations.Click or tap here to enter text.

In Indonesia, regulations related to digital transactions are still lagging behind because key regulations such as the Consumer Protection Law and the Electronic Information and Transactions Law have not fully anticipated the characteristics of digital products, including aspects of updates, conformity, and platform responsibility. Other challenges include low digital consumer literacy, weak law enforcement in cyberspace, and the absence of explicit cooling-off period regulations in digital transactions. Therefore, Indonesia needs to develop more specific regulations on digital transactions, strengthen supervisory institutions, and improve consumer literacy and protection to respond to the increasingly complex dynamics of the digital ecosystem.

Digital transactions in both countries face several challenges, such as data security, online fraud, digital literacy, and cross-border transactions. In terms of online fraud, Indonesia has seen a very worrying trend. Data from the Ministry of Communication and Information Technology recorded 572,185 cases of digital fraud from 2017 to September 2024. In addition, the Financial Services Authority (OJK) through the Indonesia Anti-Scam Center (IASC) reported public losses of Rp 3.2 trillion (approximately USD 200 million) as of June 2025, based on 157,203 public complaints. Of the total cases, 528,415 were online buying and selling fraud, while 43,770 cases were related to fictitious investments. During the period from November 2024 to January 2025 alone, losses due to cybercrime amounted to Rp 476 billion, while reports of digital fraud had exceeded 1.2 million by mid-2025. The high exposure to cybercrime is also evident from the number of digital attacks in 2023, which reached 279.84 million incidents, although this figure is down about 24% from the previous year. In the Netherlands, the problem of digital fraud is also significant but shows different characteristics. In 2024, total losses due to digital fraud are estimated to reach €1.75 billion (USD 1.94 billion), or around 0.2% of Gross Domestic Product. About 9.4% of the Dutch population reported being victims of online fraud in the same year. Furthermore, according to the European Banking Authority, the Netherlands is listed as the country with the highest rate of digital payment fraud in the EEA region, in terms of the volume of transactions indicated as fraudulent, total losses, and the overall fraud ratio.

The next challenge relates to data security. Indonesia has seen a significant increase in data breach incidents since the enactment of Personal Data Protection Law (PDP Law) No. 27 of 2022. Data shows a sharp upward trend from only 12 incidents in 2018 to 210 incidents in 2024. This surge not only indicates an escalation in cyber threats, but also reflects improvements in reporting mechanisms and transparency following the full implementation of the PDP Law in October 2024. One of the most prominent cases was the Tokopedia data breach in 2020, which affected 91 million accounts, indicating the still weak data security infrastructure of a number of digital service providers in Indonesia. Meanwhile, the Netherlands operates within the established framework of the GDPR, with strict incident reporting obligations and strong enforcement mechanisms. Every organization is required to immediately report data breaches to the Dutch Data Protection Authority and to affected individuals if there is a significant risk. A more mature, comprehensive, and certified data protection regime in the Netherlands contributes to low levels of underreporting. The fundamental difference between the two countries lies in the stage of regulatory development. Indonesia is still in the early stages of implementing strict regulations, mainly because the Personal Data Protection Agency is only projected to be fully operational in 2026, while the Netherlands already has a stable enforcement structure and a relatively high level of compliance.

The third challenge relates to digital literacy and consumer awareness. Indonesia faces a wide disparity in digital literacy, mainly due to geographical differences and access to infrastructure. Based on a 2024 study by Katadata, the digital literacy level of internet users aged 13–70 years old is at an average score of 3.47 out of 5, which is categorized as “fair to good.” At the sub-index level, information and data literacy skills are at a score of 3.17, while communication and collaboration skills are at 3.38. Interestingly, digital security and technological skills scored higher at 3.66. With internet penetration reaching 79% and users predominantly aged 16–34, the study found that younger people, who are relatively more tech-savvy, are at higher risk of online threats due to the intensity and scope of their digital activities. As part of efforts to raise consumer awareness, the National Consumer Protection Agency (BPKN) initiated the “Smart Consumer in the Digital Era” campaign in collaboration with various institutions such as OJK, Bappenas, and e-commerce associations. This program highlights the delivery of educational material through social media platforms such as YouTube, Instagram, and TikTok, with the main target audience being the younger generation. In the Netherlands, the level of digital literacy is generally very high; internet penetration reaches around 95% of the entire population, and 87% of citizens regularly make online purchases. However, high digital literacy does not fully guarantee the community's resilience to online fraud. Although 58% of Dutch people believe they are capable of recognizing fraud, this figure has actually decreased by 4% compared to the previous year. Around 43% of fraud victims expressed uncertainty as to whether artificial intelligence technology was used in the fraud, revealing a gap in public understanding of increasingly complex forms of digital fraud.

The fourth challenge relates to the dynamics of cross-border transactions. Indonesia faces a number of fundamental obstacles in providing effective protection for consumers in international e-commerce transactions. The national regulatory framework, such as Law No. 8 of 1999 on Consumer Protection and provisions in the ITE Law, is still essentially oriented towards transactions that occur within Indonesian jurisdiction. Legal protection for consumers can only be enforced against foreign businesses if they have a legal presence in Indonesia, either through a representative or branch office, or if they have met the threshold for "deemed presence," which is more than 1,000 transactions or more than 1,000 packages per year. In addition, regulatory gaps between Indonesia and its trading partners, differences in technological capacity that have implications for consumer access and protection, and the complexity of cross-jurisdictional dispute resolution mechanisms further complicate the situation. The issue of personal data protection in cross-border transactions is also an important concern. Consumers must provide personal data to make purchases from abroad, while the level of data protection in the country of origin of the platform or seller may be below Indonesian standards. National regulations on cross-border data transfers are still in the development stage, so the supervisory mechanism is not yet optimal. In contrast, the Netherlands benefits from its integration into the European Union legal system, which has established a strong harmonization framework. The GDPR applies uniformly across all member states, ensuring consistent cross-border data protection standards. The dispute resolution structure through the European Union judiciary is clearer and relatively accessible. In the context of taxation, the "reverse charge" mechanism for VAT on cross-border Business-to-Business (B2B) transactions has been clearly defined. In addition, Dutch consumers who engage in cross-border transactions within the European Union enjoy the same protections, including the right to withdraw from a transaction within 14 days, as well as the existence of easily accessible alternative dispute resolution (ADR) mechanisms.

## 4. Conclusion

This study shows that digital transformation has brought fundamental changes to the mechanisms of agreement formation and legal relationships between businesses and consumers. In the Indonesian context, digital agreements are, in principle, legally valid as long as they meet the requirements for agreements as stipulated in Article 1320 of the Civil Code, which is then reinforced through formal recognition in the ITE Law and Government Regulation No. 71 of 2019. These regulations emphasize that electronic documents, electronic contracts, and electronic signatures have the same legal force as conventional agreements. However, digital transaction practices still pose a number of challenges, such as ambiguity regarding the subject matter of the agreement, vulnerability to breach of performance, and the risk of personal data leaks. These conditions require comprehensive legal protection as guaranteed in the Consumer Protection Law, particularly regarding the right to security, comfort, honest information, and compensation mechanisms in the event of a discrepancy between goods or services and the agreement.

A comparison with the Netherlands, another country with a civil law tradition, shows that Indonesia's regulatory framework is still in its infancy. The Netherlands has implemented a more structured consumer protection regime through the integration of European Union law, including the application of Title 7.1AA DCC, the obligation of conformity of digital goods and services, the right of withdrawal within 14 days, and strict data protection standards through the GDPR. Meanwhile, Indonesia does not yet have provisions for a cooling-off period, comprehensive regulations on the conformity of digital products, or a supervisory agency that is equivalent in terms of effectiveness and independence. These differences are even more apparent in the areas of digital literacy, data security, and the handling of cross-border transactions, which remain major challenges for Indonesia.

Thus, it can be concluded that although Indonesia has provided a legal basis for the validity of digital agreements, the level of consumer protection is not as comprehensive as in the Netherlands. Strengthening digital sector regulations, increasing consumer literacy, improving dispute resolution mechanisms, and harmonizing cross-border policies are important steps to realize adaptive and effective legal protection in the digital era. This study emphasizes the need to improve norms and institutions so that the national legal system can keep pace with technological developments and ensure certainty, benefit, and fairness for consumers in digital transactions.

## Acknowledgements

First, the author would like to thank the Supervising Lecturer for providing guidance, corrections, and constructive feedback from the problem formulation stage to the final refinement of the research manuscript. The academic advice and methodological guidance provided have been an important foundation for the compilation of this research.

Veteran Law Review
Volume: 9 Issue: 1
P-ISSN: 2655-1594 E-ISSN: 2655-1608

The author also expresses appreciation to the Faculty of Law, State University of Surabaya, for providing a supportive academic environment and the necessary facilities for the research process, including access to relevant literature and legal resources.

## References

A. Amaliah Nur Abadiah Boembeng, & Amoury Adi Sudiro. (2025). Perlindungan Konsumen Transaksi Digital pada Platform E-Commerce. *Jurnal Ilmu Hukum, Humaniora, Dan Politik*.

Ade Sultan Muhammad, Salim HS, & Aris Munandar. (2020). PERJANJIAN JUAL-BELI MELALUI ELEKTRONIK (STUDI KOMPARATIF ANTARA SISTEM HUKUM INDONESIA DAN BELANDA). *Jurnal Education and Development*.

Ahmad Refi Dzuhriyan, Surya Indra Permana, & M. Khaidir Ali Gufron. (2024). *Consumer Legal Protection in Online Transactions: Challenges and Opportunities in Indonesia's Digital Economy*.

Angela Yohanna Hutagalung. (2023). THE IMPLEMENTATION OF ONLINE DISPUTE RESOLUTION IN INDONESIA'S DIGITAL ECONOMIC SECTOR (CASE STUDY: TOKOPEDIA). *Unes Law Review*.

*Attention traders and online marketplaces: new consumer legislation*. (n.d.). Retrieved December 8, 2025, from https://www.barentskrans.nl/en/publication-blogs/attention-traders-and-online-marketplaces-new-consumer-legislation/

*Consumer Protection Laws and Regulations Netherlands 2025*. (n.d.). Retrieved December 8, 2025, from https://iclg.com/practice-areas/consumer-protection-laws-and-regulations/netherlands

Deky Paryadi. (2016). *PERKEMBANGAN REGULASI PERLINDUNGAN KONSUMEN DALAM TRANSAKSI E-COMMERCE DI INDONESIA DAN NEGARA-NEGARA ASEAN*.

*Fintech Laws and Regulations 2025 – Indonesia*. (n.d.). Retrieved December 8, 2025, from https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/indonesia/

Fitmar Hebimisa, Nontje Rimbing, & Josina Emilia Londa. (n.d.). *PENEGAKAN HUKUM PERJANJIAN DALAM KONTRAK DIGITAL MENURUT UNDANG UNDANG NOMOR 11 TAHUN 2008 YANG DIBAHARUI OLEH UNDANG UNDANG NOMOR 19 TAHUN 2016*.

I Nyoman Triana Eka Putra, & Dr. I Made Dedy Priyanto, S. H. , M. K. (2025). KEABSAHAN PERJANJIAN ELEKTRONIK DALAM PERJANJIAN JUAL BELI DITINJAU DARI PRESPEKTIF HUKUM PERDATA. *JURNAL MEDIA AKADEMIK* .

*Indonesia's Updated VAT System for Cross-Border Digital Services*. (2025). https://www.aseanbriefing.com/news/indonesias-updated-vat-system-for-cross-border-digital-services

Irene Puteri Alfani Sofia Sinaga, Chionya Sherly Mahat, Grace Margareth, & Simarmata. (2024). *DINAMIKA PERJANJIAN KONTRAK ELEKTRONIK DALAM BISNIS DIGITAL: ANALISIS KOMPARATIF DAN IMPLIKASI HUKUM*.

*Laws and regulations on the market access of payment service providers*. (n.d.). Retrieved December 8, 2025, from https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/payment-institutions/licensing-requirement-for-payment-service-providers-overview/laws-and-regulations-on-the-market-access-of-payment-service-providers

*License procedure for payment services in the Netherlands*. (n.d.). Retrieved December 8, 2025, from https://www.blenheim.nl/en/blog/license-procedure-for-payment-services-in-the-netherlands/

M. Sunandar Yuwono, & Evita Isretno Israhadi. (2025). Optimization of Legal Protection for Consumers in Online Buying and Selling Transactions based on Consumer Protection Law. *Pemuliaan Keadilan*.

*Online sales and purchases (web shop)*. (n.d.). Retrieved December 8, 2025, from https://business.gov.nl/regulations/long-distance-sales-and-purchases

Rahmad Satria, Anita Yuliastini, Aleksander Sebayang, Ivan Wagner, & Yuko Fitrian. (2025). Keabsahan Perjanjian Digital dalam Transaksi

Elektronik Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Kolaboratif Sains*.

SAKTI ALAMSYAH, & FAUZIE YUSUF HASIBUAN. (2025). LEGAL PROTECTION FOR CONSUMERS IN E-COMMERCE TRANSACTIONS IN INDONESIA: CONTRACT VALIDITY AND DISPUTE RESOLUTION EFFECTIVENESS . *Pena Law International Journal of Law*.

*The New E-Commerce Regulation in Indonesia is now in Effect*. (n.d.). Retrieved December 8, 2025, from https://lokalegal.com/2023/10/20/the-new-e-commerce-regulation-is-now-in-effect

*Burgelijk Wetboek*. (n.d.).

Dutch Civil Code (2022).

General Data Protection Regulation.

Peraturan Mahkamah Agung Tentang Pengajuan Keberatan Terhadap Keputusan BPSK (2006).

Peraturan Pemerintah Tentang Pnyelenggaran Sistem Dan Transaksi Elektronik (2019).

Undang Undang ITE (2008).

Undang Undang Perlindungan Konsumen (1999).

Undang Undang Tentang Perlindungan Data Pribadi (2022).